

Escuela Politécnica Superior

19  
20

# Trabajo fin de grado

HuMI: Plataforma para la Adquisición y Modelado de Señales de Interacción Hombre-Máquina



Iván Bartolomé González

Escuela Politécnica Superior  
Universidad Autónoma de Madrid  
C/ Francisco Tomás y Valiente nº 11



**UNIVERSIDAD AUTÓNOMA DE MADRID**  
**ESCUELA POLITÉCNICA SUPERIOR**



**Grado en Ingeniería Informática**

**TRABAJO FIN DE GRADO**

**HuMI: Plataforma para la Adquisición y  
Modelado de Señales  
de Interacción Hombre-Máquina**

**Autor: Iván Bartolomé González**

**Tutor: Aythami Morales Moreno**

**Ponente: Julian Fierrez-Aguilar**

**julio 2020**

**Todos los derechos reservados.**

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución comunicación pública y transformación de esta obra sin contar con la autorización de los titulares de la propiedad intelectual.

La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (*arts. 270 y sgts. del Código Penal*).

**DERECHOS RESERVADOS**

© 3 de Noviembre de 2017 por UNIVERSIDAD AUTÓNOMA DE MADRID  
Francisco Tomás y Valiente, n.º 1  
Madrid, 28049  
Spain

**Iván Bartolomé González**

***HuMI: Plataforma para la Adquisición y Modelado de Señales de Interacción Hombre-Máquina***

**Iván Bartolomé González**

IMPRESO EN ESPAÑA – PRINTED IN SPAIN

*A mi madre, a mi familia, a mis compañeros y a mis amigos.*

*"Daría todo lo que sé, por la mitad de lo que ignoro"*

*Descartes*



# AGRADECIMIENTOS

---

En primer lugar me gustaría agradecer todo el apoyo y conocimiento que me ha aportado el grupo de investigación Biometrics and Data Pattern Analytics (BiDA-lab). En concreto a mi tutor Aythami Morales, que consiguió despertar en mi interés por los temas tratados cuando apenas estaba en tercero. Sin su conocimiento, esfuerzo, ayuda y colaboración no hubiera podido realizar este trabajo de fin de grado.

Me gustaría agradecer también a mis compañeros por haberme dado el apoyo y la ayuda necesaria para superar la carrera. En especial quería agradecer a Jose Antonio Cebrián, a Alejandro Asenjo y a Pedro Burgos por todo lo que me han aportado.

Por último, mis más sinceros agradecimientos a mi familia, en especial a mi madre, que nunca dudaron de mis capacidades y si no fuera por su paciencia, apoyo y ánimo, no hubiera sido capaz de estar aquí ahora.





# RESUMEN

---

En la actualidad, la gran parte del tráfico de internet se produce por medio de los dispositivos móviles. Esto es debido a la potencia que tienen en un tamaño reducido y a los constantes cambios en los hábitos de los usuarios que han hecho de la conectividad una "necesidad" casi constante. Este cambio de hábito hacia un tráfico basado en dispositivos móviles también se ha visto reflejado en los hábitos de los delincuentes. El uso de bots para realizar todo tipo de ataques informáticos está extendido y en los últimos años, los delincuentes han visto en los dispositivos móviles una nueva puerta de entrada. Los sistemas de detección de bots son la primera defensa ante este tipo de ataques. La mayoría de estos sistemas se basan en la resolución de tareas cognitivas (p.ej. reCAPTCHA de Google) o en el análisis de tráfico y cookies. No existen detectores de bots diseñados específicamente para el entorno móvil, capaces de aprovechar las ventajas que otorga la interacción con un dispositivo con elevado número de sensores diseñados para mejorar la interacción con ellos.

En este trabajo se detalla la creación de una plataforma de adquisición de datos de usuarios reales para el modelado de la interacción hombre-máquina en dispositivos móviles. Dicha plataforma constará de un total de 17 pruebas con las que se pueda caracterizar las capacidades cognitivas y neuromotoras del usuario. Con esta plataforma se espera obtener una base de datos completa en cuanto al número de sensores con la que crear modelos. Como la base de datos contiene información sensible de los usuarios en algunas pruebas, un proceso de anonimización se llevará a cabo antes de la publicación. Esta base de datos, "HuMI", procedente de "Human Mobile Interaction", será analizada con el fin de poder visualizar sus características y desarrollo temporal y comparada con las existentes, viendo las ventajas y desventajas de esta. Esta base de datos se utilizará para modelar la interacción hombre-máquina en dispositivos móviles y desarrollar una nueva generación de detectores de bots basados en ella.

Adicionalmente, en el marco experimental se plantea una simplificación de la creación de usuarios artificialmente por medio de Redes Generativas Antagónicas (GANs) para demostrar el potencial que puede ofrecer la base de datos obtenida. Con estos modelos generados se podrán evaluar modelos reales, aunque será necesario un análisis cuantitativo de las muestras.

# PALABRAS CLAVE

---

Dispositivos móviles, bots, plataforma, interacción hombre-máquina, base de datos, redes neuronales, GANs, modelos, análisis.



# ABSTRACT

---

Nowadays, much of the Internet traffic is carried by mobile devices. This is due to the power they have in a small size and the constant changes in user habits that have made connectivity an almost constant "need". This shift to mobile-based traffic has also been reflected in the habits of criminals. The use of bots to carry out all kinds of computer attacks is widespread and in recent years, criminals have seen mobile devices as a new gateway. Bot detection systems are the first defense against this type of attack. Most of these systems are based on the resolution of cognitive tasks (e.g. Google reCAPTCHA) or on the analysis of traffic and cookies. There are no bot detectors designed specifically for the mobile environment, capable of taking advantage of interaction with a device with a high number of sensors designed to improve interaction with them.

In this work, we detail the creation of a platform for the acquisition of real user data for the modelling of human-machine interaction in mobile devices. This platform will consist of a total of 17 tests with which the cognitive and neuromotor capacities of the user can be characterized. With this platform it is expected to obtain a complete database in terms of the number of sensors and create models with it. As the database contains sensitive information from users in some tests, an anonymisation process will be carried out before publication. This database, "HuMI", coming from "Human Mobile Interaction", will be analysed in order to visualize its characteristics and temporal development and compared with the existing ones, seeing the advantages and disadvantages of it. This database will be used to model the human-machine interaction in mobile devices and to develop a new generation of bot detectors based on it.

Additionally, in the experimental framework, a simplification of the creation of users artificially by using Antagonistic Generative Networks (GANs) is proposed in order to demonstrate the potential that the obtained database can offer. With these generated models it will be possible to evaluate real models, although a quantitative analysis of the samples will be necessary.

# KEYWORDS

---

Mobile devices, bots, platform, human-machine interaction, database, neural networks, GANs, models, analysis.



# ÍNDICE

---

<b>1</b>	<b>Introducción</b>	<b>1</b>
1.1	La importancia de los dispositivos móviles .....	1
1.2	Motivación .....	2
1.3	Objetivos .....	3
1.4	Organización .....	4
1.5	Contribuciones de este TFG .....	4
<b>2</b>	<b>Tecnologías de detección de bots</b>	<b>5</b>
<b>3</b>	<b>Desarrollo de una App de Captura de Interacción Hombre-Dispositivo</b>	<b>9</b>
3.1	Privacidad .....	10
3.2	Sistema de Ficheros .....	10
3.3	Sistema de control Global .....	11
3.4	Sistema de control de Sesiones .....	12
3.5	Keystroke .....	13
3.6	Scroll-Up y Scroll-Down .....	14
3.7	Touch .....	15
3.8	Air_X y Air_O .....	16
3.9	Voz .....	17
3.10	Números .....	18
3.11	Envío .....	19
<b>4</b>	<b>HuMI: Base de Datos para Modelado de Interacción Hombre-Máquina</b>	<b>21</b>
<b>5</b>	<b>Modelado Sintético de Interacción de Usuarios</b>	<b>27</b>
<b>6</b>	<b>Conclusiones y trabajo futuro</b>	<b>31</b>
6.1	Conclusiones .....	31
6.2	Trabajo futuro .....	31
	<b>Bibliografía</b>	<b>34</b>



# LISTAS

---

## Lista de figuras

1.1	Número de dispositivos móviles vendidos de 2007 a 2020. Fuente: [1] .....	1
2.1	CAPTCHA: Texto predefinido .....	5
2.2	CAPTCHA: Selección por imágenes/puzles .....	6
2.3	CAPTCHA: Puzle de 4 piezas .....	6
2.4	CAPTCHA: Puzle complejo .....	7
2.5	CAPTCHA: Google V2 .....	7
3.1	Diagrama de flujo de la aplicación .....	9
3.2	Diagrama UML sobre la clase GlobalData .....	12
3.3	Diagrama UML sobre la clase Sesion y dependencias .....	13
3.4	Prueba de dinámica de tecleo. ....	13
3.5	Prueba de deslizamiento de contenido .....	15
3.6	Prueba de pulsación .....	15
3.7	Prueba neuromotora .....	16
3.8	Prueba de audio .....	17
3.9	Pruebas numéricas manuscritas .....	18
4.1	Avance temporal de usuarios nuevos .....	21
4.2	Distribución del número de sesiones de los usuarios .....	22
4.3	Distribución de género .....	22
4.4	Distribución de la edad .....	23
4.5	Distribución de la edad completa .....	23
4.6	Distribución de localizaciones .....	24
4.7	Dispositivos sin sensores .....	25
4.8	Dispositivos con sensores .....	25
4.9	Visualización de los datos obtenidos. Fuente [2] .....	26
5.1	Diagrama de la red .....	27
5.2	Ejemplo de trazo sintético y real .....	28
5.3	Perfiles de Aceleración de los trazos .....	29
5.4	Suavizado de la señal real .....	29

## Lista de tablas

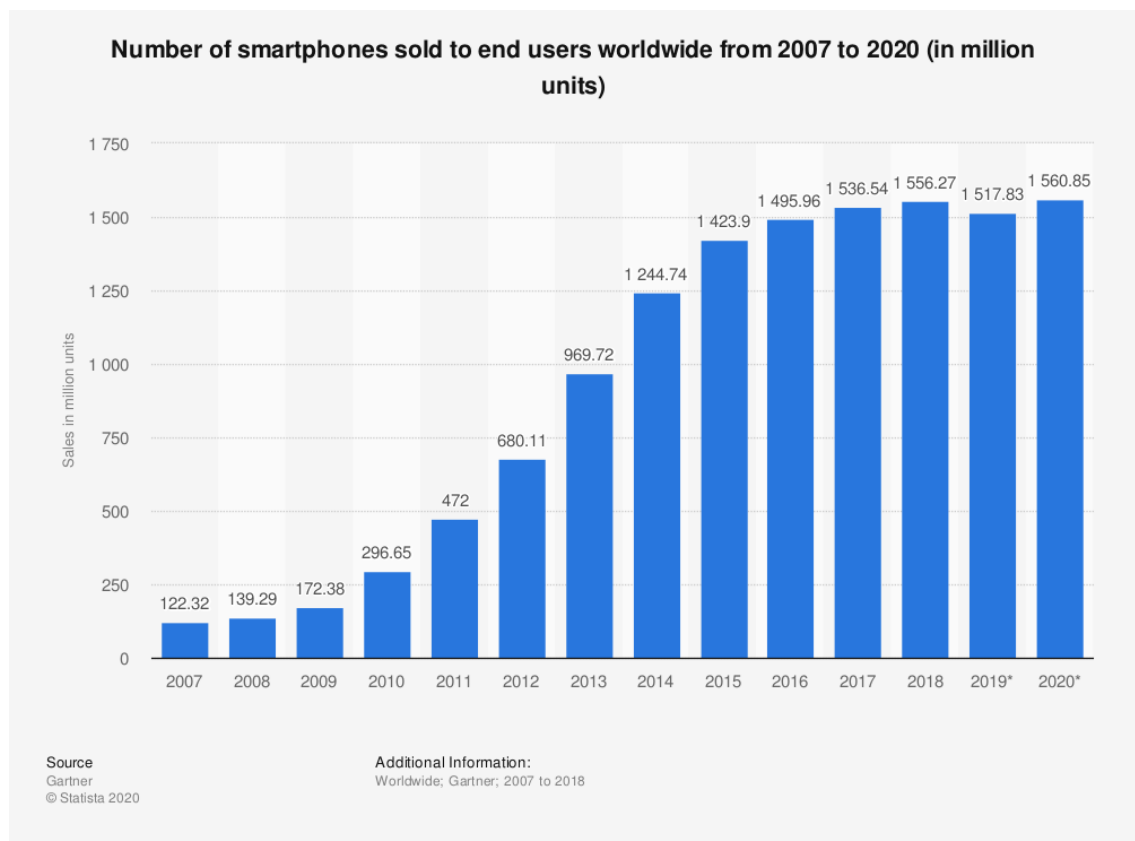
1.1	Bases de datos de dispositivos móviles . . . . .	3
3.1	Sensores recogidos en HuMI . . . . .	11
3.2	Valores del campo ID_CAMPO en el fichero . . . . .	14
3.3	Valores del campo CODE en el fichero . . . . .	15
4.1	Dispositivos destacados . . . . .	24



# INTRODUCCIÓN

## 1.1. La importancia de los dispositivos móviles

Durante los últimos años, el número de dispositivos móviles ha crecido rápidamente y esto es debido a la increíble capacidad tanto de cómputo como de almacenamiento que tienen para ser dispositivos de tan reducido tamaño. Podemos ver el aumento de ventas [1] en la figura 1.1.



**Figura 1.1:** Número de dispositivos móviles vendidos de 2007 a 2020. Fuente: [1].

Así mismo, en la actualidad se estima que hay 4.78 Billones de dispositivos en el mundo, lo que supone un 61.51 % de la población mundial como podemos ver en [3].

Dado el potencial de estos dispositivos, hay multitud de líneas de investigación que aprovechan los distintos datos que estos pueden proporcionar. Podemos encontrar investigaciones basadas en autenticación de usuarios [4], en la monitorización de comportamientos [5] y de la salud [6].

Sin embargo, estos dispositivos también han cambiado el comportamiento de los usuarios, proporcionando nuevos modos de acceso a internet o de creación de contenido. Estudios recientes revelan que el 72.6 % del tráfico de internet se producirá mediante dispositivos móviles para 2025. Actualmente, cerca del 51 % del acceso a internet se hace por esta vía. [7]

El hecho de tener tantos dispositivos móviles crea un riesgo potencial, ya que el software malicioso también se adapta a los dispositivos móviles. Un claro ejemplo es el uso de bots en los dispositivos, afectando a multitud de servicios como redes sociales (creación de cuentas falsas para propagar información falsa o con fines maliciosos), ataques DDoS o incluso afectando a las apuestas financieras.

Inicialmente, los bots se limitaban a tareas sencillas como hacer click en un lugar de la pantalla. Sin embargo cada vez son más sofisticados, siendo capaces de realizar tareas que antes solo estaban al alcance de los humanos, como puede ser el reconocimiento de imágenes, procesamiento de texto o incluso audio.

Viendo tanto los pros como los contras de los dispositivos móviles nos hace preguntarnos si podemos encontrar diferencias entre la interacción generada por un usuario real y la interacción generada por un bot. Para ello, deberíamos definir un modelo de usuario capaz de distinguir entre los dos tipos de usuarios. Sin embargo, para crear dicho modelo, necesitaríamos disponer de una base de datos con los distintos sensores del dispositivo, además de los datos obtenidos en determinadas acciones.

## 1.2. Motivación

Uno de los aspectos que ha motivado la realización de este trabajo ha sido la gran presencia de bots en la sociedad actual, teniendo en cuenta la cantidad de dispositivos móviles presentes y futuros como hemos podido ver en la sección 1.1.

Existen sistemas CAPTCHAS (ej. ReCAPTCHA de Google) desarrollados para entornos webs y su uso es común desde hace años. La mayoría de estos sistemas se basan en pruebas cognitivas o de análisis de tráfico web. No obstante, estos sistemas no explotan la información generada durante la interacción con dispositivos móviles.

Existen artículos como [8] donde usan uno de los sensores de los dispositivos móviles (acelerómetro) para calcular el pulso de un usuario. Podemos ver en [9] que también son capaces de estimar el pulso por medio de la cámara del móvil o incluso en [10] se puede relacionar los síntomas depresivos con los datos de los sensores.

Viendo el potencial que tiene el análisis de la información de los dispositivos nos da que pensar cual es el límite al que se puede llegar con estos datos. Esta es la principal motivación de la creación de una base de datos con el mayor número de sensores posibles para futuros estudios sobre el comportamiento humano.

En la tabla 1.1 mostraremos las bases de datos más importantes cuyo fundamento es el mismo que la base de datos de este TFG.

Ref.	Sensores	Usuarios	Sesiones por Usuario	Dispositivo
[11]	13 (Key, Cam, Tou, Gyr, Acc, Mag, Lig, GPS, Blu, WiF, Pro, Tem, Pres)	54	~248	Compartido
[12]	2 (WiF, Acc)	312	1 Mes	Propio
[13]	2 (Acc, Gyr)	304	~90	Propio
[14]	3 (App, Web, GPS)	200	5 Meses	Propio
[15]	5 (Tou, Pow, Acc, Gyr, Mag)	10	3 Horas	Compartido
[16]	4 (Acc, Gyr, Mag, Ori)	102	20 - 50 Días	Compartido
[17]	8 (Key, GPS, Acc, Gyr, Mag, Acc, Gra, Rot)	37	15 Días	Propio
[18]	3 (Touch, Acc, Gyr)	217	≤6	Propio

**Tabla 1.1:** Bases de datos de dispositivos móviles.

Como podemos observar, disponemos de varias bases de datos pero hay algunos inconvenientes. En [11], aunque es una base de datos bastante completa, tenemos pocos usuarios, aunque se compensa con la cantidad de sesiones por usuario. Sin embargo, que se obtuviera de un mismo dispositivo puede afectar al comportamiento de los individuos. Se puede observar que la mayoría de las bases de datos vistas tienen pocos sensores o, teniendo un gran número de sensores tiene pocos usuarios. Por ello nos basaremos en los sensores de [11] para la base de datos a capturar.

Si queremos modelar la interacción hombre-máquina necesitaremos de una base de datos con elevado número de usuarios (para modelar el comportamiento), elevado número de dispositivos (interoperabilidad de sensores) y un elevado número de sensores (que permitan explorar nuevas tecnologías).

## 1.3. Objetivos

El objetivo principal de este trabajo es la creación de una plataforma de adquisición de los datos necesarios para el modelado de la interacción hombre-máquina por medio de los sensores de un dispositivo móvil.

Con la plataforma creada, el siguiente objetivo es la adquisición de una base de datos, denominada "HuMI" (Human Mobile Interaction), a partir de dicha plataforma que permita modelar la interacción de usuarios reales con los dispositivos móviles.

El siguiente objetivo a considerar es la creación de usuarios sintéticos mediante Generative Adversarial Networks (GANs) [19] y comparar los datos obtenidos con los datos reales, viendo si después somos capaces de clasificar el tráfico entre usuarios reales y artificiales.

## 1.4. Organización

En primer lugar se expone el estado del arte en el ámbito de las bases de datos con los datos de los sensores de los dispositivos móviles.

En segundo lugar, se muestra el planteamiento y desarrollo de la plataforma de captura de datos, siendo esta una aplicación Android con varias pruebas.

Una vez la captura se realizó, seguimos con la explicación de la base de datos obtenida, así como la distribución de usuarios y sus datos.

A continuación realizamos experimentos de generación de patrones partiendo de únicamente un patrón de comportamiento de los usuarios y, por último, se concluye el trabajo con los trabajos realizados con la base de datos y propuestas de trabajos futuros.

## 1.5. Contribuciones de este TFG

Como resultado de este TFG, se ha participado en la publicación de 1 artículo científico y una patente:

- A Acien, A Morales, J Fierrez, R Vera-Rodriguez, I Bartolome, "Be-CAPTCHA: Detecting Human Behavior in Smartphone Interaction using Multiple Inbuilt Sensors," Proc. of AAAI Workshop on Artificial for Cyber Security (AICS), New York, USA, 2020.

- Aythami Morales, Julian Fierrez, Ruben Vera-Rodriguez, Javier Ortega-García, Alejandro Acien Ayala, Ruben Tolosana Moranchel, Iván Bartolomé Gonzalez. MÉTODO PARA GENERAR DATOS DE ENTRENAMIENTO DE UN MÓDULO DETECTOR DE BOTS, MÓDULO DETECTOR DE BOTS ENTRENADO A PARTIR DE LOS DATOS DE ENTRENAMIENTO GENERADOS MEDIANTE EL MÉTODO Y SISTEMA DE DETECCIÓN DE BOTS. Spanish Patent Application P202030066. Fecha de solicitud: 28/01/2020

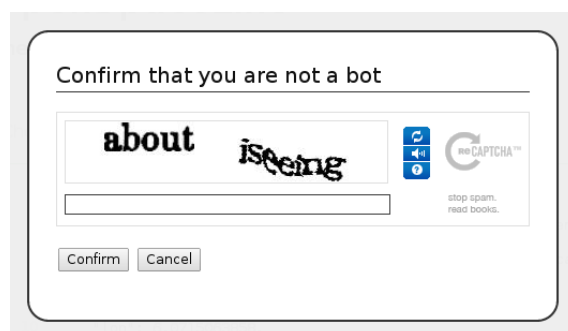
También se ha creado un repositorio público a través del cual compartir la base de datos generada:

<https://github.com/BiDALab/HuMIdb>

## TECNOLOGÍAS DE DETECCIÓN DE BOTS

Inicialmente se planteó la detección de bots con la prueba de Turing o 'test de Turing'. Esta prueba consistía en un examen de la capacidad de una máquina tiene para tener un comportamiento similar o indistinguible a un ser humano. Las primeras pruebas que propuso Alan Turing fue que un humano evaluara la conversación en lenguaje natural entre un humano y una máquina diseñada para generar respuestas similares a la de un humano.

Los sistemas de detección de bots actuales usados en el acceso web somenten a los usuarios a distintas pruebas cognitivas. A este mecanismo se le denominó CAPTCHA (cuyas siglas son "Completely Automated Public Turing test to tell Computers and Humans Apart"). Una de las primeras pruebas utilizadas para la detección de bots en la web se basaba en introducir un conjunto de caracteres mostrados en una imagen levemente distorsionada (como podemos ver en la figura 2.1), de modo que no había un sistema de aprendizaje, únicamente una comparación de lo esperado con lo introducido por el usuario.



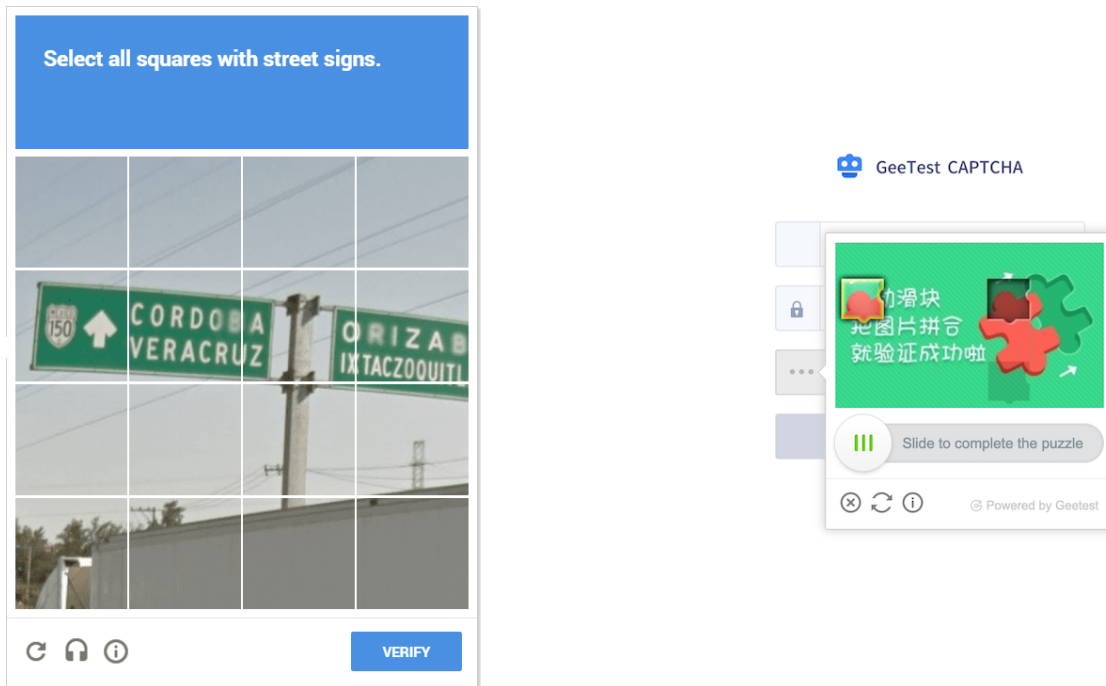
**Figura 2.1:** CAPTCHA: Texto predefinido.

Posteriormente, se introdujeron nuevos sistemas de reconocimiento basados en imágenes, que consistía en la división de una imagen en cuadrículas donde el usuario tenía que seleccionar las celdas en las que se encontraba el objeto. Sin embargo, gracias a los avances en el reconocimiento automático de objetos, la efectividad de este sistema se está viendo afectada.

También se introdujeron algunos sistemas de reconocimiento basados en puzzles o juegos, como principio de la "gamificación", donde el usuario tenía que resolver algún tipo de rompecabezas, como

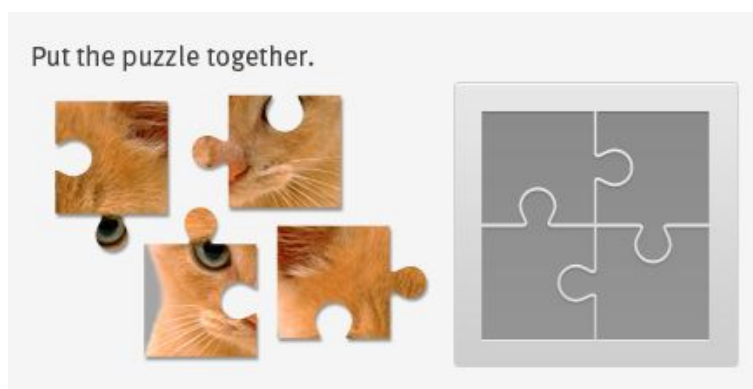
por ejemplo GeeTest CAPTCHA. En este debías deslizar un botón hasta hacer coincidir la pieza con un hueco. Una ventaja de este sistema es que no dispone de un tipo de aprendizaje o calculo específico, lo que lo hace menos vulnerable que el mencionado anteriormente.

Podemos ver un ejemplo de estos últimos métodos en la figura 2.2, donde a la izquierda tenemos la selección de señales y a la derecha un puzzle simple a resolver.



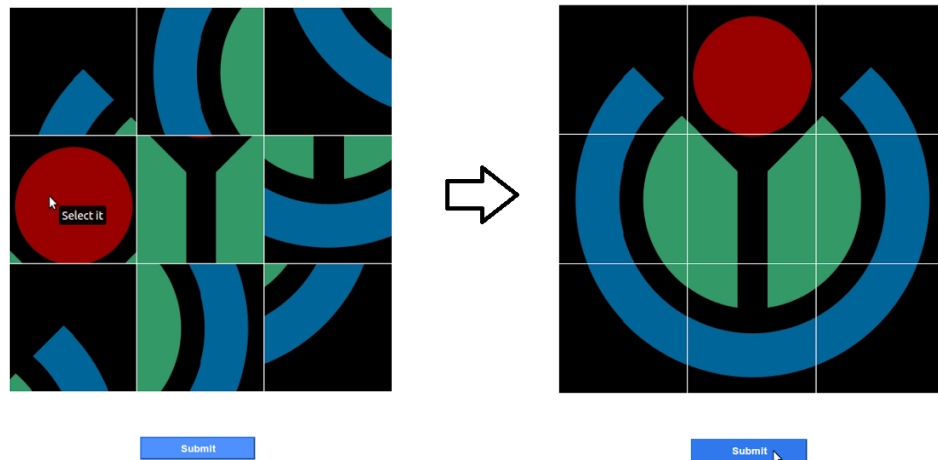
**Figura 2.2:** CAPTCHA: Selección por imágenes/puzzles.

La complejidad de los puzzles se fue incrementando con el fin de dificultar a los bots el resolverlos. Se crearon puzzles de pocas piezas, normalmente 4 como vemos en la figura 2.3, que debías colocar ordenadas.



**Figura 2.3:** CAPTCHA: Puzzle de 4 piezas.

Sin embargo, la complejidad de los puzles aumentó de tal modo que hasta resultaban complejos para los humanos por no entender que se esperaba de las pruebas. Un ejemplo es la prueba de la figura 2.4, donde a simple vista no se puede intuir la forma final de la imagen.



**Figura 2.4:** CAPTCHA: Puzle complejo.

En los últimos años surgieron nuevos mecanismos de reconocimiento de bots basados en el comportamiento o la conducta de los usuarios. En este campo, destacamos el CAPTCHA de Google, que tiene 3 versiones distintas:

- reCAPTCHA v1: Actualmente no se utiliza.
- reCAPTCHA v2: Botón de 'No soy un robot', como vemos en la figura 2.5.
- reCAPTCHA v3: Análisis del comportamiento en segundo plano.



**Figura 2.5:** CAPTCHA: Google V2.

Recientemente se han desarrollado métodos de detección de bot por las trayectorias generadas por la interacción de los usuarios con el ratón en la web como podemos ver en [20]. Como este TFG prioriza la explotación de los sensores de los dispositivos móviles.

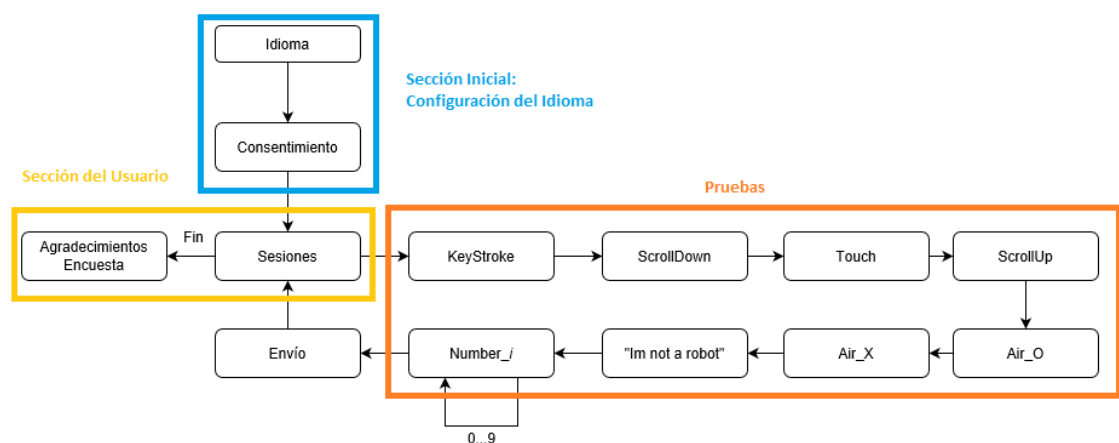




# DESARROLLO DE UNA APP DE CAPTURA DE INTERACCIÓN HOMBRE-DISPOSITIVO

En primer lugar, se planteó un diseño de varias pruebas a realizar hasta que se decidió que cada sesión tendría un total de 17 pruebas, de las cuales 10 serían para la obtención de los números manuscritos del 0 al 9 respectivamente. Las otras 7 pruebas consistirían en la obtención de la dinámica de tecleo (keystroke), dos pruebas del deslizamiento de contenido en la pantalla (scroll) tanto hacia arriba como hacia abajo, una prueba de tocar botones (Touch), dos pruebas de movimiento libre del dispositivo (Air\_X y Air\_O) y por último una prueba de voz, en la cual el usuario deberá decir “Im not a Robot” o “No soy un robot”. Con estas pruebas se busca caracterizar las capacidades cognitivas y neuromotras del usuario. A su vez, permitirán modelar la interacción del usuario con el dispositivo en diferentes escenarios de uso.

El diagrama de flujo en la figura 3.1 de la aplicación entonces quedaría tal que así:



**Figura 3.1:** Diagrama de flujo de la aplicación.

Ahora procederemos a detallar la implementación del sistema de gestión y de cada prueba, así como el resultado final de cada una y finalizaremos con el envío de datos, mencionando al final la última pantalla donde se agradece la participación y se muestra un formulario.

## 3.1. Privacidad

Un aspecto muy importante a la hora de desarrollar una plataforma para la adquisición de los datos de los usuarios es la privacidad de esta respecto a la información que se recopila.

Teniendo en cuenta que la aplicación obtiene una gran cantidad de información sensible, es necesaria una política de privacidad explícita sobre el tipo de información recopilada, así como su tratamiento, como podemos ver en [21].

Para ello, se procesará la base de datos resultante con el fin de anonimizar estos o borrar los usuarios indebidos (como los menores de 13 años). Este proceso se aplicará en los audios obtenidos de las pruebas y en la primera prueba de la dinámica de tecleo. Se explicará el proceso de anonimizar cada prueba en su apartado correspondiente.

Sin embargo, este proceso se hará a posteriori de la adquisición de la información debido al alto coste computacional del método en algunas pruebas y podría interferir en el comportamiento de los usuarios, variando la información obtenida.

## 3.2. Sistema de Ficheros

Para almacenar los distintos usuarios sin incluir datos privados en el identificador, se ha optado por utilizar la MAC de los dispositivos como identificador, de modo que al final tendremos una carpeta con una “u” seguida de la MAC. Sin embargo, para garantizar el anonimato, la MAC será eliminada a en la fase de anonimizado, siendo sustituida por un identificador numérico.

Dentro de cada carpeta de usuario, tendremos un mínimo de 1 carpeta y un máximo de 5 carpetas pertenecientes a las sesiones, así como un fichero con la información de cada usuario (idioma, resolución de la pantalla, MAC, modelo del dispositivo...).

Cada sesión estará subdividida en 17 carpetas, con los nombres vistos en la figura X, así como 3 ficheros con los dispositivos WiFis, Bluetooth y posición GPS.

Las carpetas pertenecientes a cada prueba comparten 2 archivos (swipe.csv, el cual muestra el desplazamiento para pasar a la siguiente prueba, y micro.3pg, que contiene lo grabado en la prueba. Adicionalmente, también comparten una subcarpeta con los sensores que capturamos (Gravedad, Giroscopio, Humedad, Acelerómetro normal/lineal, Luz, Magnetómetro, Proximidad y Temperatura).

Podemos ver la frecuencia de muestreo de cada sensor, así como los datos obtenidos y el consumo del sensor en la siguiente tabla:

Sensores	Frecuencia de muestreo	Características	Consumo
Accelerometer	200 Hz	x,y,z	Bajo
L.Accelerometer	200 Hz	x,y,z	Bajo
Gyroscope	200 Hz	x,y,z	Bajo
Magnetometer	200 Hz	x,y,z	Bajo
Orientation	NA	l o p	Bajo
Proximity	NA	cm	Bajo
Gravity	NA	m/s <sup>2</sup>	Bajo
Light	NA	lux	Bajo
TouchScreen	E	x,y,p	Medio
Keystroke	E	key, p	Medio
GPS	NA	Lat., Lon., Alt., Bearing, Accuracy	Medio
WiFi	NA	SSID, Level, Info, Channel, Frequency	Alto
Bluetooth	NA	SSID, MAC	Medio
Microphone	8 KHz	Audio	Alto

**Tabla 3.1:** Sensores recogidos en HuMI.

### 3.3. Sistema de control Global

Para implementar este sistema, se ha recurrido al uso del patrón Singleton, de manera que únicamente haya una instancia de la clase que se encarga del control global de la aplicación y se ha declarado la clase **GlobalData**.

Como la aplicación se planteó para poder mostrarse en dos idiomas distintos (inglés y español), la variable definida como lenguaje se guarda en la primera pantalla de selección de idioma y esta es la que establece el idioma de la aplicación cambiando la configuración con un tipo de datos "Locale" definido en las clases de Android.

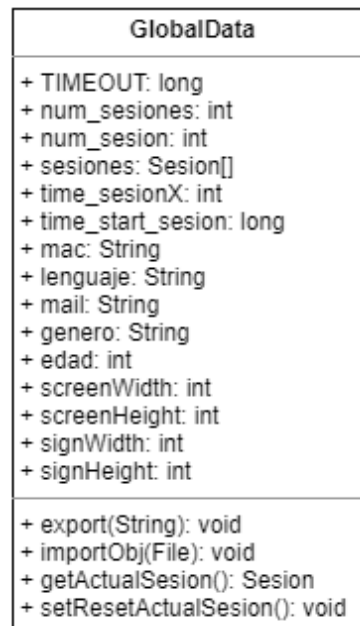
Para controlar las distintas sesiones en las que se divide el periodo de muestreo, esta clase contiene un array de sesiones, que explicaremos más adelante, el número de sesiones máximas y el número de la sesión actual, así como el tiempo que debe pasar entre cada sesión.

Por motivos de eficiencia, los datos referentes al dispositivo, tales como la MAC y las dimensiones de la pantalla y espacio de adquisición de los números manuscritos, se guardan también en esta clase.

Del mismo modo que los datos referentes al usuario, como veremos en el apartado de keystroke, se guardan de forma temporal hasta el envío de la sesión.

Con el fin de mantener el control de las sesiones, la persistencia de datos es importante, de modo que se definen los métodos de guardar y cargar el objeto (serializando este objeto), así como un

método de exportación de los datos en modo texto, el cual se guardará con las sesiones.



**Figura 3.2:** Diagrama UML sobre la clase GlobalData.

### 3.4. Sistema de control de Sesiones

Al iniciar la aplicación, se carga el objeto con el método `importObj` de `Global data`, y entonces se carga la pantalla de las sesiones, para eso, disponemos de un array con las 5 sesiones que contiene la prueba.

Cada Sesión a su vez está compuesta por los distintos desplazamientos para la siguiente prueba, uno por cada prueba, listas de los datos de cada prueba y tres listas de la posición GPS, de los dispositivos WiFi y de los dispositivos BlueTooth. Adicionalmente, esta clase es la encargada de la exportación de los datos al finalizar cada sesión para posteriormente proceder al envío al servidor.

Dado que es un sistema compuesto por varias sesiones, se decidió que fueran sesiones diarias, es decir, que entre sesiones hubiera mínimo 24 horas con el fin de darle variabilidad a las condiciones en las que se realizan las pruebas. De modo que, para facilitar a los usuarios que recuerden que tienen una sesión disponible que hacer, se implantó un sistema de notificaciones, el cual muestra una notificación en la barra de notificaciones del dispositivo móvil. Este sistema se carga al iniciar el móvil y, en caso de borrar la notificación, se volverá a notificar en el plazo de 24 horas.

Debido a que se están tomando una gran cantidad de sensores, para evitar colapsar el servidor, se limita el tiempo máximo por sesión a 5 minutos, de modo que si se emplea más tiempo durante la sesión se notificará y no se enviarán los datos.

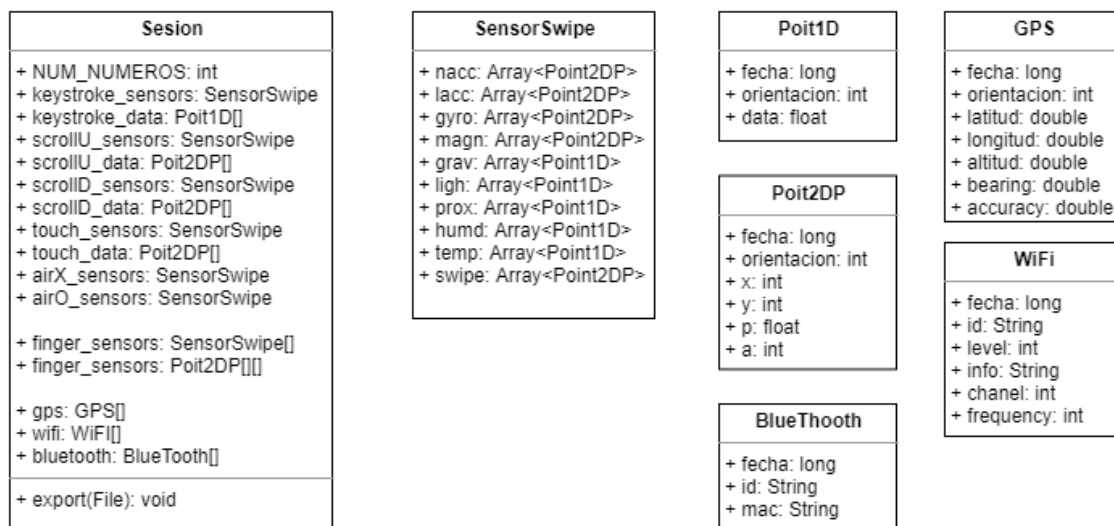


Figura 3.3: Diagrama UML sobre la clase Sesion y dependencias.

## 3.5. Keystroke

La primera prueba planteada en la aplicación tiene como finalidad el análisis de la dinámica de tecleo de cada usuario. Para ello, dentro de la misma prueba se plantean dos tipos de campos para rellenar: un campo cuyo contenido es variable en cada usuario (nombre, apellidos, edad y género), de modo que tenemos unos datos sin supervisar y un campo con el contenido predefinido, siendo este "En un lugar de la mancha de cuyo nombre no quiero acordarme". Podemos ver la prueba en la figura 3.4.

Figura 3.4: Prueba de dinámica de tecleo.

La manera en la que el sistema guarda la información sobre los campos viene definida por un observador de eventos denominado `TextChangedListener`, el cual recibe un objeto que definimos como "CustomTextWatcher" que implementa la interfaz "TextWatcher".

Esta clase guarda los cambios en los campos de texto de la prueba en un fichero con el siguiente formato:

**"timestamp ID\_CAMPO ASCII\_CODE"**

El valor del ID\_CAMPO se puede observar en la tabla 3.2.

ID	Valor
N	Nombre
S	Apellidos
A	Edad
T	Texto Predefinido

**Tabla 3.2:** Valores del campo ID\_CAMPO en el fichero.

Como mencionamos anteriormente en el apartado de la privacidad, esta información es de carácter sensible y es necesario anonimizarla, de modo que la información obtenida en los campos de nombre, apellidos y edad se suprimirá el ASCII\_CODE de los caracteres por un valor común, ya que únicamente nos interesa la dinámica de tecleo más que el contenido.

## 3.6. Scroll-Up y Scroll-Down

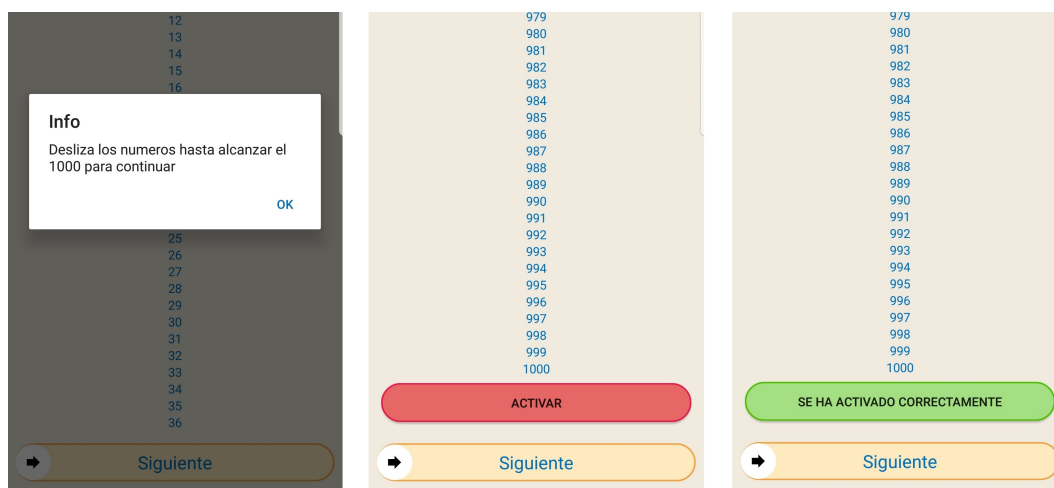
Las dos siguientes pruebas consisten en un análisis de los patrones de desplazamiento de contenido de los usuarios. Para ello, se han diseñado dos pruebas con el fin de analizar el deslizamiento tanto vertical como horizontal de una lista de 1000 números. Al final de la lista, una vez alcancemos el valor máximo, tendremos un botón que activar para poder continuar con la siguiente prueba. Podemos ver la prueba en la figura 3.5.

La importancia de esta prueba reside en los trazos que cada individuo realiza sobre el dispositivo para cambiar el contenido. Esto simula un entorno donde el usuario dispone de mucho contenido y tiene que navegar por él, como podría ser un artículo o un periódico web.

La manera en la que el sistema guarda la información viene definida por un observador de eventos sobre la vista de la prueba. Se registra el momento temporal en el que se produce el evento, la posición (x,y), la presión con la que se pulsó y el tipo de evento.

Esta clase guarda la información de la prueba en un fichero con el siguiente formato:

**"timestamp orientación X Y presión CODE"**



**Figura 3.5:** Prueba de deslizamiento de contenido.

El valor del CODE se puede observar en la tabla 3.3.

ID	Valor
0	Pulsación inicial
1	Pulsación final
2	Pulsación mantenida

**Tabla 3.3:** Valores del campo CODE en el fichero.

## 3.7. Touch

La siguiente prueba consiste en una colección de 6 botones que inicialmente aparecerán en rojo y se deberán ir tocando para activarlos, pasando a ser verdes. No se podrá avanzar a la siguiente prueba sin haber activado todos los botones y no se podrá activar un botón sin seguir el patrón de desbloqueo. El botón que puede ser activado tendrá el texto resaltado en negrita. Podemos ver la prueba en la figura 3.6.



**Figura 3.6:** Prueba de pulsación.

Como la activación de los botones siguen la misma secuencia entre las sesiones, la primera sesión del usuario nos proporcionará más información referente a la velocidad de reacción y a los reflejos (tiempo de reacción al recibir un estímulo, el cual es la activación de un botón tras pulsar el inicial). Mientras que las siguientes sesiones se acentuará la memoria muscular del individuo.

La manera en la que el sistema guarda la información sobre el comportamiento viene definida por un observador de eventos sobre la vista de la prueba y sobre cada uno de los botones. Se registra el momento temporal en el que se produce el evento, la posición (x,y), la presión con la que se pulsó y el tipo de evento. Justo como en la prueba anterior.

Esta clase guarda la información de la prueba en un fichero con el siguiente formato:

**"timestamp orientación X Y presión CODE"**

El valor del CODE se puede observar en la tabla 3.3 vista en la prueba anterior.

### 3.8. Air\_X y Air\_O

En las dos siguientes pruebas se debe mover el dispositivo móvil haciendo un círculo y una cruz en el aire. Podemos ver las pruebas en la figura 3.7.



**Figura 3.7:** Prueba neuromotora.

La importancia de esta prueba reside en ver la capacidad neuromotora de los usuarios en un entorno 3D sin límites, sometiéndoles a las pruebas en un entorno libre y dando solo la indicación de la figura. De este modo podemos analizar tanto las distintas interpretaciones posibles que los usuarios puedan dar a las imágenes, como el tipo de movimiento que estos hacen: un movimiento rápido y decidido, uno lento y dubitativo...

La manera en la que el sistema guarda la información está principalmente en los sensores, haciendo hincapié en el acelerómetro y giroscopio. De esa manera podemos también analizar cómo han movido el dispositivo a la hora de hacer la forma (rotación, velocidad, etc.).



## 3.9. Voz

La siguiente pruebas consisten en una pantalla donde grabar una frase con el micrófono. Disponemos de tres botones: uno para comenzar la grabación, otro reproducir la grabación (si esta existe), y un último para parar la grabación. En el caso de existir una grabación y presionar el botón de grabar de nuevo, se sobrescribirá la existente. Podemos ver las pruebas en la figura 3.8.



**Figura 3.8:** Prueba de audio.

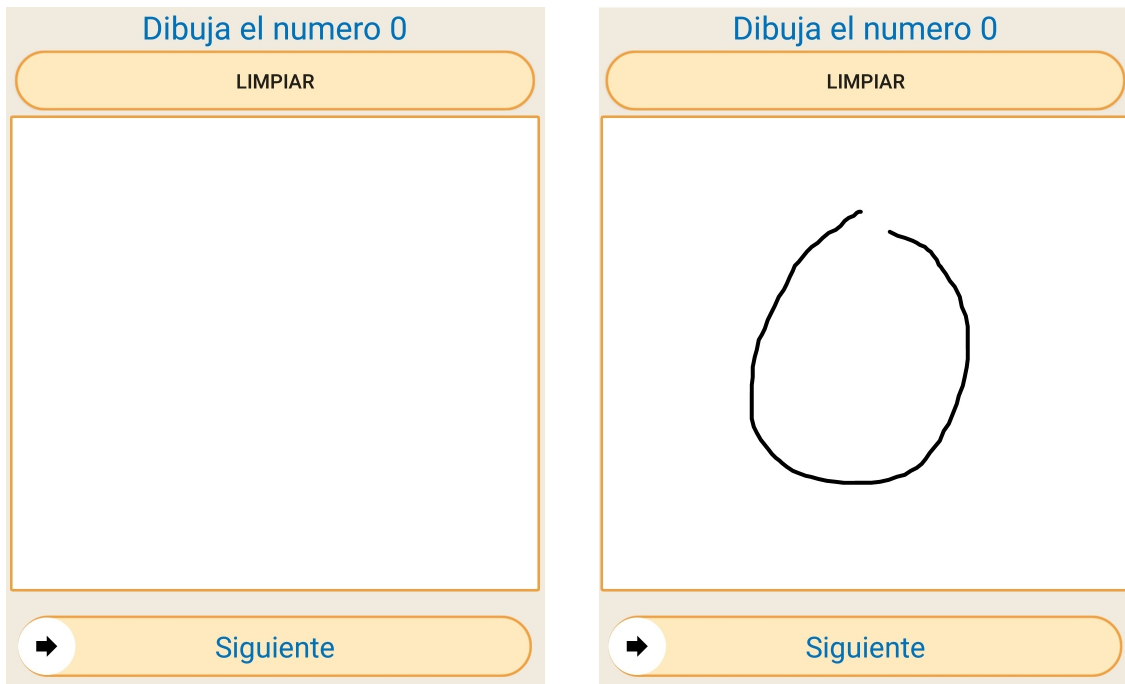
Antes de ver la motivación de la prueba, tenemos que tener en cuenta que la información que contienen los ficheros de audio puede ser sensible. Por eso mismo, y como mencionamos en el apartado de privacidad, debemos procesar estos archivos para quedarnos con la información relevante sin interferir con la privacidad de los usuarios.

La importancia de esta prueba reside obtener la caracterización vocal de los usuarios al pronunciar las palabras "No soy un robot" o "I'm not a robot". El resto de la información del audio, se debe procesar para obtener únicamente la energía o envolvente de archivo con el fin de obtener el contexto en el que fue grabado. Con esto, podríamos clasificar los distintos usuarios en función del contexto en el que se hicieron las pruebas.

La manera en la que el sistema guarda la información está principalmente en el archivo de audio con la extensión "3gp".

### 3.10. Números

La última prueba se compone de 10 pantallas donde el usuario debe escribir los números del 0 al 9 con el dedo. Se dispone de un botón con el que borrar el número y empezar de nuevo. Podemos ver una de las pantallas, con el número 0 en la figura 3.9.



**Figura 3.9:** Pruebas numéricas manuscritas.

Como podemos ver en la base de datos [18], esta se compone tanto de números como de caracteres manuscritos. Eso fue una motivación para crear estas pruebas, con el fin de recopilar una base de datos numéricos manuscritos con un mayor número de sensores.

La manera en la que el sistema guarda la información donde se escribe se obtiene por un observador de eventos sobre el canvas. Se registra el momento temporal en el que se produce el evento, la posición (x,y), la presión con la que se pulsó y el tipo de evento. Justo como en la prueba anterior.

Esta clase guarda la información de la prueba en un fichero con el siguiente formato:

**"timestamp orientación X Y presión CODE"**

El valor del CODE se puede observar en la tabla 3.3 vista en la sección 3.6.

## 3.11. Envío

Una vez se han completado todas las pruebas y recopilado la información de manera local, se procede a hacer el envío de los datos.

Para elegir el proceso de envío de la información se plantearon diversos métodos. En primer lugar se pensó en tener un servidor dedicado en el que guardar todo. Sin embargo, este método era muy costoso ya que no se disponía de un servidor con una IP pública fija. En el caso de utilizar un equipo dentro de la Universidad Autónoma de Madrid, se debería instalar un servicio de VPN para poder enviar los datos. Este método se descartó debido a que no todos los usuarios tendrían cuenta en la VPN o conocimientos para conectarse.

El método elegido entonces fue utilizar Firebase como servidor de alojamiento. Firebase a su vez ofrece funcionalidad que confirma el envío de la información. Este servicio proporcionado por Google es gratuito, sin embargo, se tuvo que aumentar la tarifa debido a la cantidad de información de los usuarios.

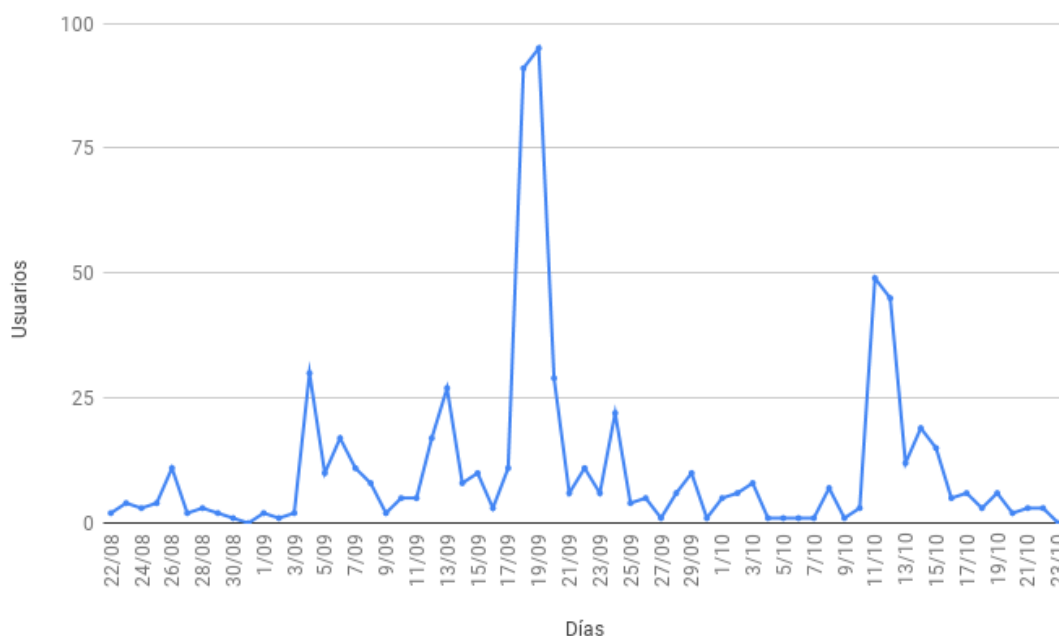
Para cada envío de cada sesión, se comprime todo en un único fichero ZIP y se intenta enviar contra el servidor de Firebase. En el caso de que se envíe correctamente, se aumenta el contador de la sesión actual y se programa la notificación de la siguiente sesión. En el caso de no enviarse correctamente, se informa y no se incrementan los contadores con el fin de sobrescribirse al hacer la siguiente sesión.

Cuando se completan todas las sesiones, se muestra una encuesta que podemos observar en [22] o su versión inglesa en [23].



# HuMI: BASE DE DATOS PARA MODELADO DE INTERACCIÓN HOMBRE-MÁQUINA

La plataforma para la adquisición de los datos se publicó el 22 de Agosto de 2019 y el periodo de recogida de la información duró dos meses, finalizando el día 23 de Octubre de 2019. Podemos ver el avance del número de usuarios nuevos por día en la figura 4.1.

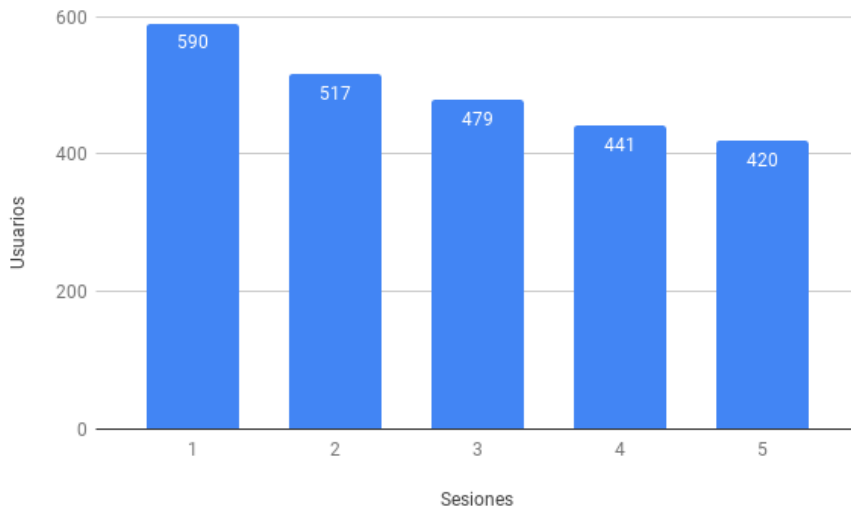


**Figura 4.1:** Avance temporal de usuarios nuevos.

Como se puede observar, se comenzó con pocos usuarios en las primeras dos semanas. No fue hasta el día 3 de Agosto donde hubo un incremento de 30 usuarios, pasando de 37 a 67. Las siguientes dos semanas fueron un poco inestables, teniendo una media de 11 usuarios por día.

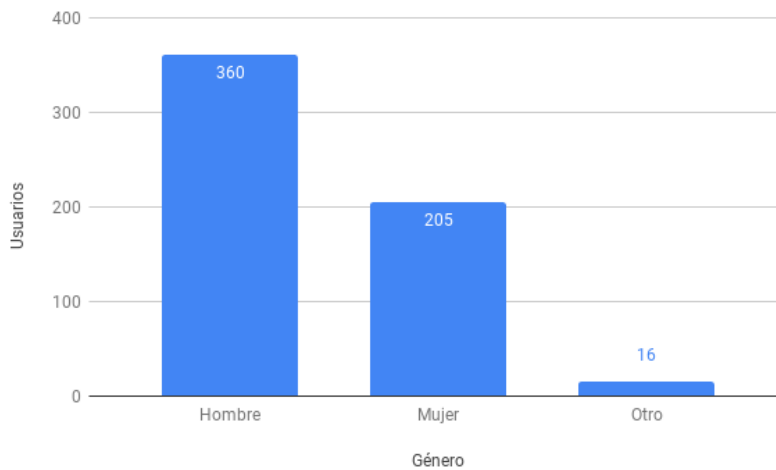
Los días 17 y 18 de Agosto hubo un incremento de 91 y 95 usuarios, siendo estos en su mayoría de Ecuador. Las siguientes 3 semanas no hubo un incremento sustancial de usuarios, teniendo una media de 6 nuevos usuarios por día. No fue hasta el día 10 de Octubre donde hubo otra subida de usuarios, teniendo 49 nuevos usuarios. Pero eso fue decreciendo hasta el día 23 que ya no hubo ningún nuevo usuario, coincidiendo con el periodo de fin de toma de datos.

Tras eliminar los usuarios indebidos, nos quedamos con un total de 590 usuarios. Sin embargo, no todos los usuarios tienen las 5 sesiones. Podemos ver la distribución del número de sesiones de los usuarios en la tabla 4.1.



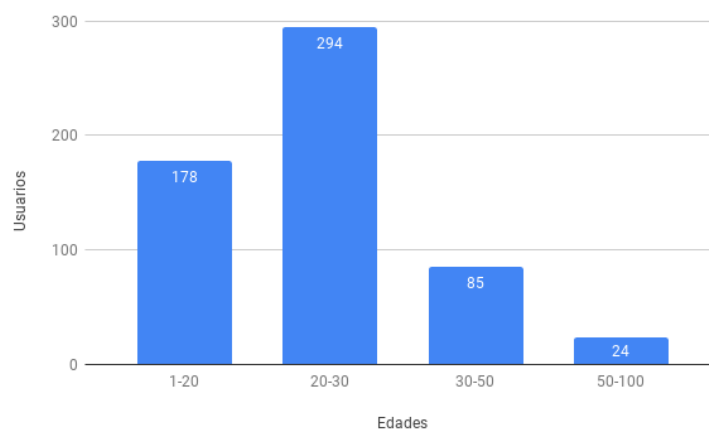
**Figura 4.2:** Distribución del número de sesiones de los usuarios.

Ahora es necesario fijarse en las características de la base de datos, empezando por una división en cuanto al género. Podemos ver la distribución en la figura 4.3. En esta podemos observar que el 61.96 % de los usuarios son hombres, el 35.28 % son mujeres y el 2.76 % se corresponde a otro.



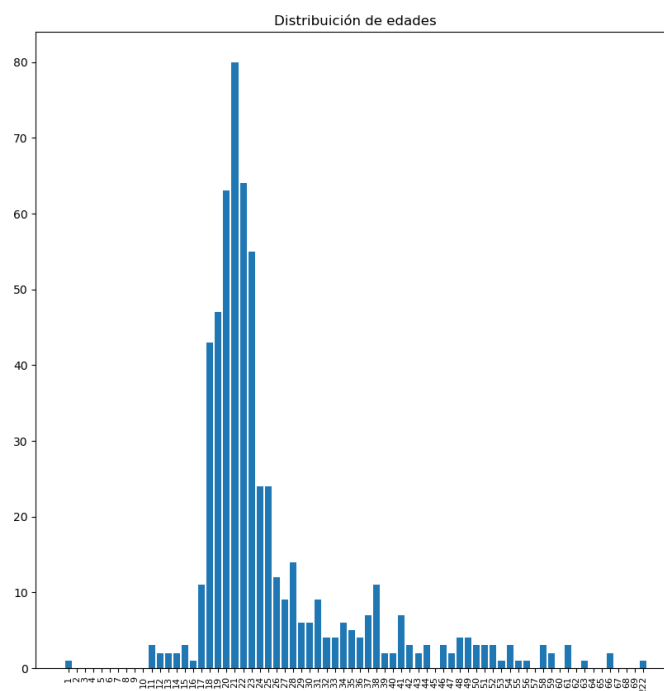
**Figura 4.3:** Distribución de género.

Si nos fijamos en la distribución de la edad, podemos ver que en la figura 4.4 que la franja dominante es la que se encuentra entre 20 a 30 años, siendo esta un 50.6 % de los usuarios, seguida del 30.63 % de los menores de 20 años. Los mayores de 30 años pero menores de 50 son un 14.63 % y los mayores de 50 un 4.14 %.



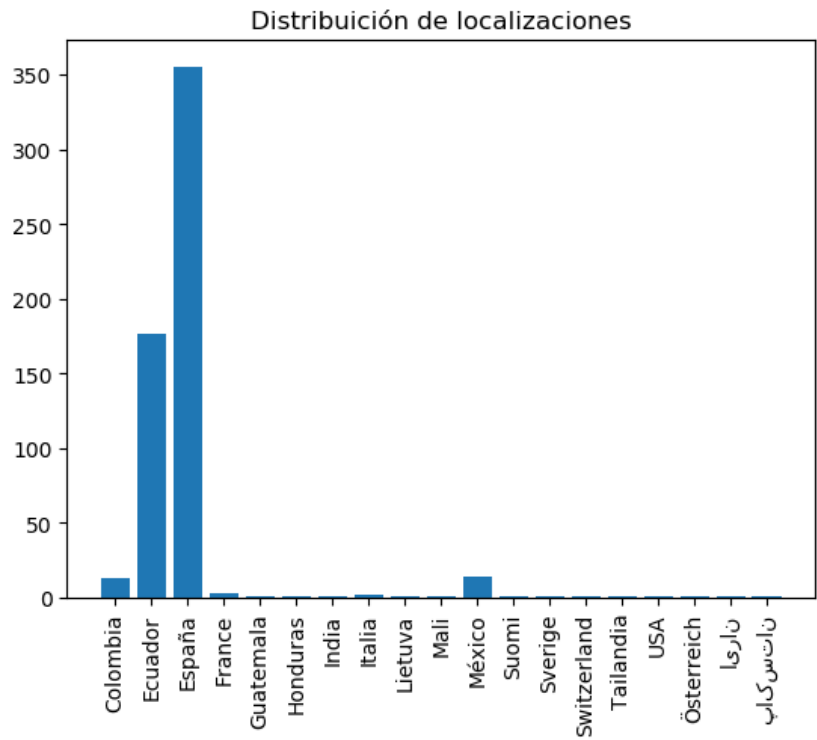
**Figura 4.4:** Distribución de la edad.

Podemos ver una distribución binomial centrada en la franja de 20a 30 años, pero para comprobarlo, nos fijaremos en la figura 4.5, donde ahora si vemos claramente este modelo centrado en 21.



**Figura 4.5:** Distribución de la edad completa.

Como mencionamos anteriormente, hubo un pico de usuarios nuevos procedentes de Ecuador, de modo que vamos a hacer un análisis de las localizaciones de los usuarios. Para ello nos fijamos en la figura 4.6. Como se puede observar, tenemos principalmente 4 países que engloban a la totalidad de usuarios. En primer lugar está España, con 355 usuarios, seguido de Ecuador con 177 usuarios y al final Colombia y México con 13 y 14 usuarios respectivamente. El resto de países tienen 2 o menos usuarios, haciendo un total de 18 usuarios en conjunto.



**Figura 4.6:** Distribución de localizaciones.

Como definimos en el estado del arte, la mayoría de las bases de datos estaban bajo un mismo dispositivo, de modo que parece interesante analizar los distintos dispositivos donde los usuarios hicieron las pruebas.

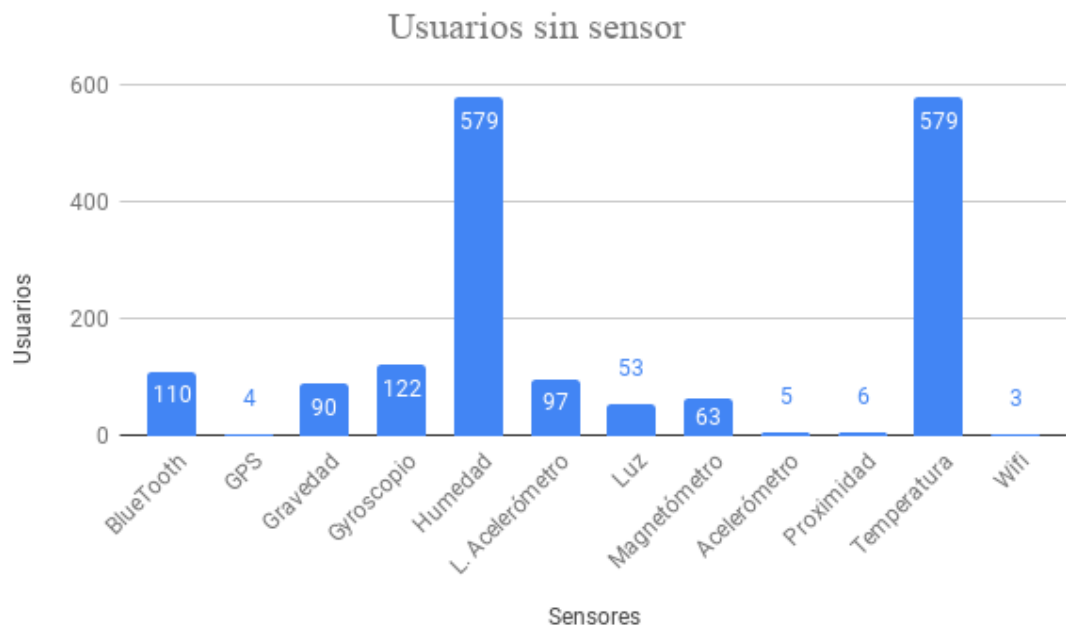
Tras el análisis, pudimos observar que hay 224 dispositivos distintos, pero podemos ver en la tabla 4.1 los 5 dispositivos más comunes, que hacen un total de 88 dispositivos, englobando un 15.14 %.

Dispositivo	Cantidad
Redmi Note 7	22
Mi A2 Lite	19
Mi A1	19
Redmi Note 5	15
SM-G930F	13

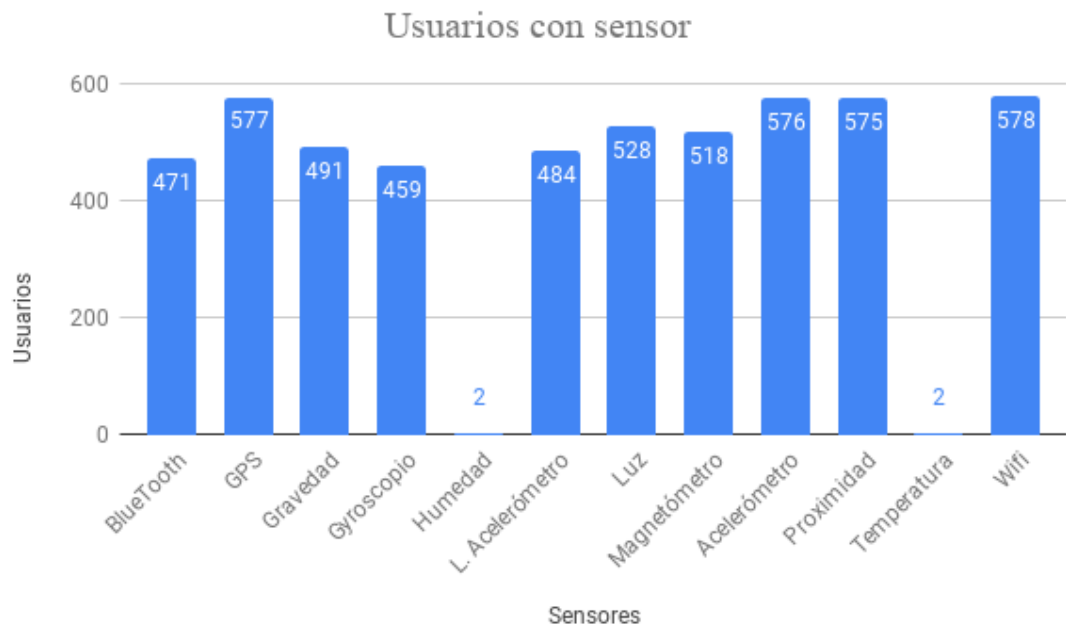
**Tabla 4.1:** Dispositivos destacados.

Finalmente, viendo la diversa cantidad de dispositivos, deberíamos tener en cuenta que no todos los dispositivos tienen todos los sensores, de modo que veremos en la figura 4.7 cuantos usuarios no disponen de cada sensor y en la figura 4.8 veremos los cuantos si disponen del sensor, siendo esta tabla la complementaria de la anterior.



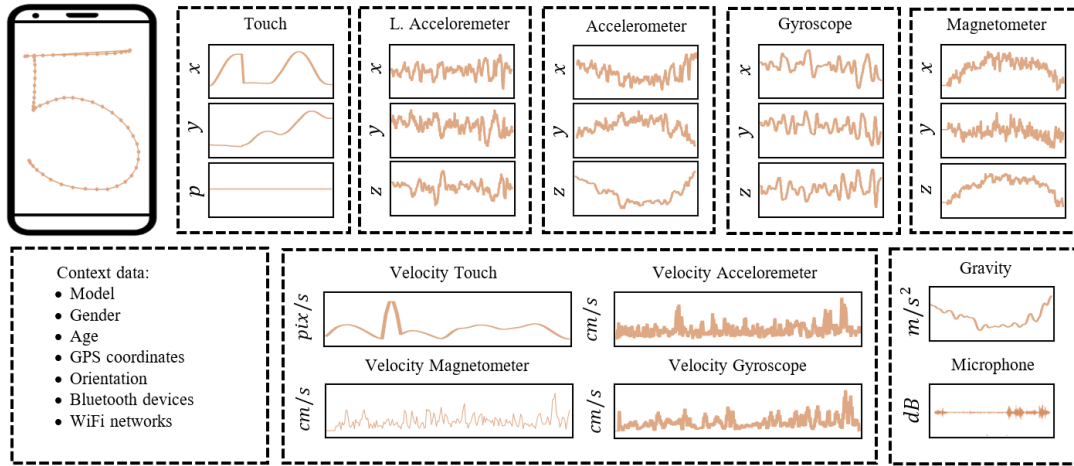


**Figura 4.7:** Dispositivos sin sensores.



**Figura 4.8:** Dispositivos con sensores.

La figura 4.9 muestra como un simple gesto realizado sobre la pantalla táctil se puede modelar a través de diferentes señales de naturaleza heterogénea. Esta riqueza de sensores permite abordar el desarrollo de modelos más complejos y difíciles de atacar.



**Figura 4.9:** Visualización de los datos obtenidos. Fuente [2].

# MODELADO SINTÉTICO DE INTERACCIÓN DE USUARIOS

Una vez se ha conseguido el primer objetivo (generación de la base de datos), el siguiente objetivo es la sintetización de muestras para evaluar los distintos modelos generados mediante el análisis de los usuarios.

En los últimos años, gracias al incremento de la capacidad de cómputo de los equipos, se han empezado a usar las denominadas Redes Generativas Antagónicas, también denominadas como GANs en inglés. Se trata de un sistema de dos redes neuronales, con aprendizaje no supervisado, que compiten entre sí (llamadas Generador y Discriminador) en un juego de suma cero. Este algoritmo de inteligencia artificial ha tenido un gran impacto y aplicaciones como FaceApp han conseguido crear imágenes sintéticas que no parecen ser creadas artificialmente.

En los siguientes experimentos, intentaremos generar mediante este algoritmo de aprendizaje trazos sintéticos con el fin de simular el deslizamiento del botón para pasar entre pruebas, denominado Swipe. Para ello, generaremos trazos sintéticos mediante el generador a partir de ruido generado aleatoriamente. Este trazo sintético, junto con los datos reales de Swipe de los usuarios, serán administrados al Discriminador, el cual intentará crear un modelo que clasifique entre datos reales y falsos. De modo que competirán entre sí para ir generando cada vez trazos más realistas a la vez que el discriminador irá mejorando en distinguirlos. Podemos ver el diagrama en la figura 5.1.

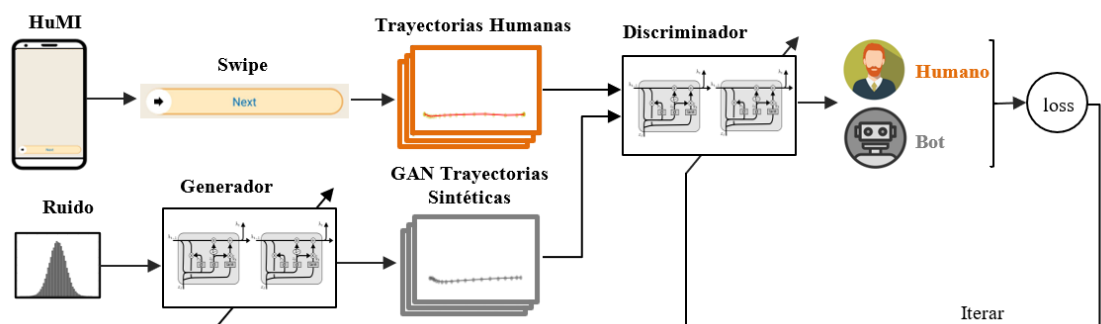
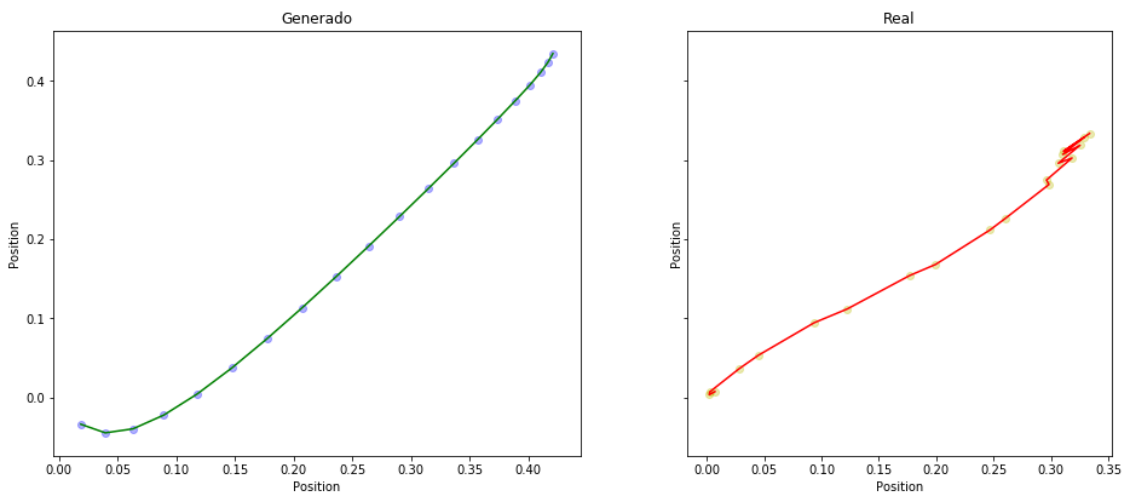


Figura 5.1: Diagrama de la red.

Para ver la capacidad de estas redes, plantemos un experimento con 30 usuarios, de los cuales obtendremos un trazo por usuario. Para simplificar el problema, usaremos las coordenadas, x e y, de los trazos como datos de entrenamiento sin tener en cuenta otro datos como la presión o el momento temporal en el que se tomó la muestra. Como los trazos no tienen una longitud definida, se deberá normalizar a una longitud fija además de normalizar los valores de los datos respecto a la resolución de la pantalla. Entrenaremos con 16 épocas y un batch size de 10.

El discriminador estará compuesto de dos redes LSTM bidireccionales de 32 y 16 unidades respectivamente, seguidos de dos conjuntos de capas densas con una activación LeakyReLU. Estas capas densas tendrán 32 y 16 neuronas. Para finalizar tendremos una capa densa con una neurona que será la clasificación final. Para el generador, tendremos dos capas LSTM de 128 y 64 unidades.

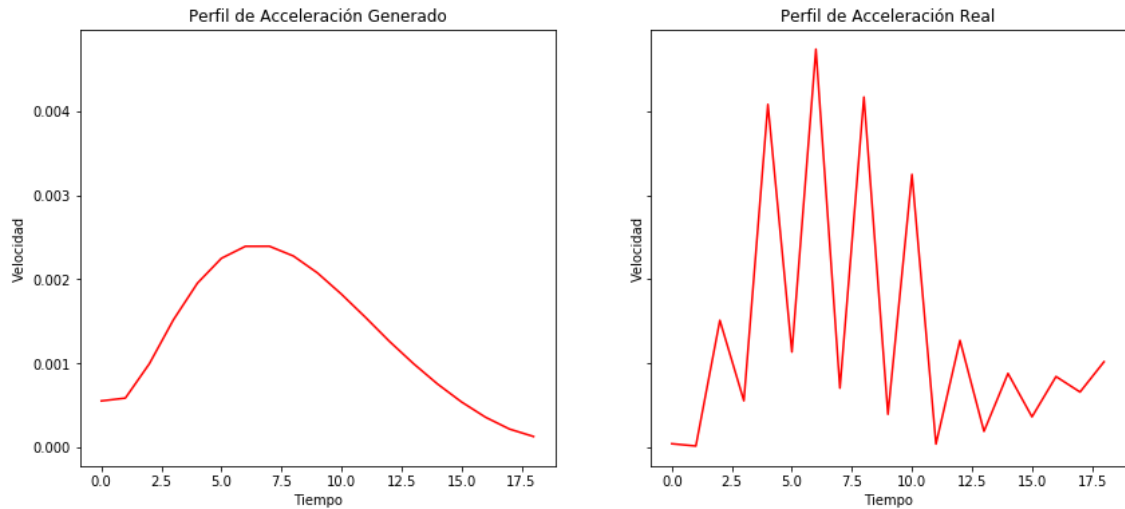
Podemos ver un ejemplo de un trazo generado por el generador y uno real en la figura 5.2.



**Figura 5.2:** Ejemplo de trazo sintético y real.

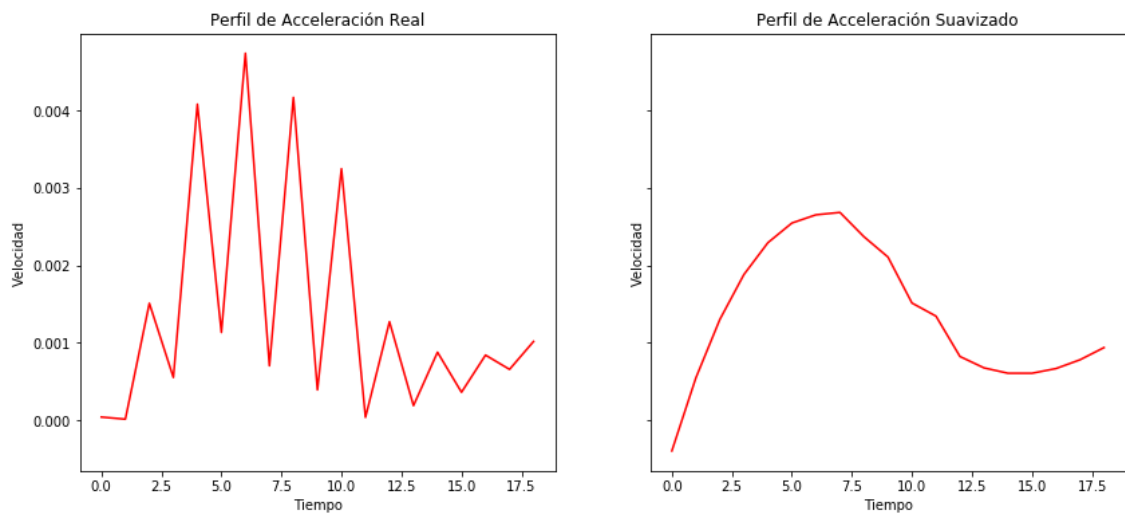
Hay que tener en cuenta que los trazos a sintetizar son sencillos y en su mayoría lineales. Pero un trazo no está definido solamente por su trayectoria espacial. Para modelar la capacidad neuromotora del usuario, es clave el análisis de la información temporal de la secuencia. En este sentido, la velocidad y aceleración dará gran información acerca de esta interacción. La teoría de los movimientos rápidos humanos [24] explica como un modelo realizado con la mano implica la actuación de dos grupos de músculos agonistas y antagonistas. Estos músculos permitirán la aceleración inicial y la desaceleración final del movimiento. Esto se verá reflejada como una rápida aceleración al inicio del trazo (muestras más juntas), una velocidad alta en mitad (muestras separadas) y una desaceleración al final (muestras más juntas al final).

Podemos ver en la figura 5.3 los perfiles de aceleración de los trazos de la figura 5.2. Se puede observar que ambos trazos siguen la teoría de los movimientos rápidos de [24] aunque el perfil sintético está más suavizado que el real.



**Figura 5.3:** Perfiles de Aceleración de los trazos.

Debido al ruido que tiene la señal, es necesario homogenizar la señal. Para ello se usa la función Savitzky–Golay de suavizado, cuyo efecto se puede observar en la figura 5.4. Ahora se puede observar la similitud existente entre el perfil suavizado y el perfil generado sintéticamente.



**Figura 5.4:** Suavizado de la señal real.

Este experimento solo muestra el potencial de la base de datos capturada y el método de generación propuesto. Para validar que las muestras sintéticas son lo suficientemente realista, el trabajo futuro requerirá de un análisis cuantitativo de estas muestras.



## CONCLUSIONES Y TRABAJO FUTURO

---

### 6.1. Conclusiones

En este Trabajo de Fin de Grado se ha creado una plataforma para recopilar información de la interacción hombre-máquina. Sin embargo, al ser una aplicación Android y estar disponible en multitud de dispositivos, se han tenido que solventar problemas que surgían en dispositivos donde no se habían realizado las pruebas subiendo una nueva versión con los cambios a la plataforma. La plataforma, finalmente, queda satisfactoriamente publicada en Google Play para seguir recopilando información y corregir futuros errores.

Hoy en día, hay diversas bases de datos con la misma finalidad que HuMI. Sin embargo, esta es de las primeras que tienen un número considerable de usuarios teniendo en cuenta los 14 sensores de los que se recopila información y que dispositivo se ha utilizado para ello. Teniendo un total de 224 dispositivos distintos frente a un único dispositivo utilizado en una base de datos con un número similar de sensores. Esta base de datos puede ser tener mucha importancia en el futuro, pudiendo ser un referente a futuras bases de datos en dispositivos con un mayor número de sensores. HuMI queda compuesta por casi 600 usuarios pero en un futuro se ampliará con usuarios nuevos.

Además, se presenta un método de generación de usuarios simplificado como ejemplo de las posibilidades que ofrece la base de datos. Los resultados son bastante buenos para la simplicidad de la prueba, generando trazos simples basados en la posición. Sin embargo, usar pocos usuarios para la prueba puede repercutir negativamente al rendimiento al producirse un sobreajuste a los datos.

### 6.2. Trabajo futuro

Como trabajo futuro se presenta una ampliación del número de usuarios de la base de datos, ya que el periodo de adquisición de datos fue de solo dos meses. Con esto tendríamos compensaríamos las 5 sesiones con más usuarios. Otra posibilidad sería aumentar el número de pruebas para analizar aspectos que en este Trabajo Fin de Grado no se han podido abordar. Un ejemplo de prueba podría ser de equilibrio, usando el móvil como balanza.

También se propone hacer un análisis cuantitativo de la información con el fin de mejorar el método de generación de nuevos usuarios pero esta vez incluyendo la dependencia temporal y los sensores del dispositivo.



# BIBLIOGRAFÍA

---

- [1] "Smartphones sold to end users worldwide from 2007 to 2020." <https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/>. Accessed: 2020-06-01.
- [2] A. Acien, A. Morales, R. Vera-Rodriguez, and J. Fierrez, "Smartphone sensors for modeling human-computer interaction: General outlook and research datasets for user authentication," 06 2020.
- [3] "How many smartphones are in the world?." <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world>. Accessed: 2020-06-01.
- [4] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking touchscreen biometrics for mobile authentication," *IEEE Trans. on Information Forensics and Security*, vol. 13, pp. 2720–2733, November 2018.
- [5] L. Pei, R. Chen, J. Liu, T. Tenhunen, H. Kuusniemi, and Y. Chen, "Inquiry-based bluetooth indoor positioning via rssi probability distributions," *2010 Second International Conference on Advances in Satellite and Space Communications*, pp. 151–156, 2010.
- [6] M. V. Albert, S. Á. de Toledo, M. Shapiro, and K. P. Kording, "Using mobile phones for activity recognition in parkinson's patients," *Frontiers in Neurology*, vol. 3, 2012.
- [7] "Almost three quarters of internet users will access via their smartphones by 2025." <https://www.cnbc.com/2019/01/24/smartphones-72percent-of-people-will-use-only-mobile-for-internet-by-2025.html>. Accessed: 2020-06-01.
- [8] S. Kwon, J. Lee, G. S. Chung, and K. S. Park, "Validation of heart rate extraction through an iphone accelerometer," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5260–5263, 2011.
- [9] P. Pelegris, K. Banitsas, T. Orbach, and K. Marias, "A novel method to detect heart beat rate using a mobile phone," in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*, pp. 5488–5491, 2010.
- [10] S. Saeb, M. Zhang, C. J. Karr, S. M. Schueller, M. E. Corden, K. P. Kording, and D. C. Mohr, "Mobile phone sensor correlates of depressive symptom severity in daily-life behavior: An exploratory study," *J Med Internet Res*, vol. 17, p. e175, Jul 2015.
- [11] U. Mahbub and R. Chellappa, "Path: Person authentication using trace histories," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pp. 1–8, 2016.
- [12] G. Li and P. Bours, "Studying wifi and accelerometer data based authentication method on mobile phones," in *Proceedings of the 2018 2nd International Conference on Biometric Engineering and*

- Applications*, ICBEA '18, (New York, NY, USA), p. 18–23, Association for Computing Machinery, 2018.
- [13] G. Li and P. Bours, “A novel mobilephone application authentication approach based on accelerometer and gyroscope data,” in *2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–4, 2018.
- [14] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, “Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location,” *IEEE Systems Journal*, vol. 11, no. 2, pp. 513–521, 2017.
- [15] X. Liu, C. Shen, and Y. Chen, “Multi-source interactive behavior analysis for continuous user authentication on smartphones,” in *CCBR*, 2018.
- [16] Y. Lin, S. Cheng, J. Shen, and M. Pantic, “Mobiface: A novel dataset for mobile face tracking in the wild,” pp. 1–8, 05 2019.
- [17] D. Deb, A. Ross, A. K. Jain, K. O. Prakah-Asante, and K. V. Prasad, “Actions speak louder than (pass)words: Passive authentication of smartphone users via deep temporal features,” *CoRR*, vol. abs/1901.05107, 2019.
- [18] R. Tolosana, J. Gismero-Trujillo, R. Vera-Rodríguez, J. Fierrez, and J. Ortega-Garcia, “Mobile-touchdb: Mobile touch character database in the wild and biometric benchmark,” *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 2306–2314, 2019.
- [19] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in *Advances in Neural Information Processing Systems 27* (Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, eds.), pp. 2672–2680, Curran Associates, Inc., 2014.
- [20] A. Acien, A. Morales, J. Fierrez, and R. Vera-Rodriguez, “Becaptcha-mouse: Synthetic mouse trajectories and improved bot detection,” *ArXiv*, vol. abs/2005.00890, 2020.
- [21] “Política de privacidad de humi.” <http://atvs.ii.uam.es/atvs/licencia.html>. Accessed: 2020-06-20.
- [22] “Encuesta final de humi.” [https://docs.google.com/forms/d/1ChXA\\_NOMOF6JHnWnmkvXEnQbFdZmp5za37eQKNut3uU/edit?usp=sharing](https://docs.google.com/forms/d/1ChXA_NOMOF6JHnWnmkvXEnQbFdZmp5za37eQKNut3uU/edit?usp=sharing). Accessed: 2020-06-20.
- [23] “Encuesta inglesa final de humi.” [https://docs.google.com/forms/d/108h73veDPyc1a03r6jpsGKD7O6NsRST-88\\_b00cHrKU/edit?usp=sharing](https://docs.google.com/forms/d/108h73veDPyc1a03r6jpsGKD7O6NsRST-88_b00cHrKU/edit?usp=sharing). Accessed: 2020-06-20.
- [24] R. Plamondon, “A kinematic theory of rapid human movements. part ii. movement time and control,” *Biological cybernetics*, vol. 72, pp. 309–20, 02 1995.



